The Algebraic Properties of Formal Group Laws

Shay Ben Moshe

20/06/2017

1 Motivation

Let k be an algebraically closed field. We can look at $G_m = \operatorname{Spec}\left(k\left[x, x^{-1}\right]\right) \cong k^*$, where the elements are $\mathfrak{m}_a = (x - a)$ for $a \in k^*$, it has the structure of an algebraic group, given by a map $G_m \times G_m \to G_m$, $(\mathfrak{m}_a, \mathfrak{m}_b) \mapsto \mathfrak{m}_{ab}$. Under the (contravariant) spectrum functor, it comes from $k\left[z, z^{-1}\right] \to k\left[x, x^{-1}\right] \otimes k\left[y, y^{-1}\right] = k\left[x, x^{-1}, y, y^{-1}\right]$, $z \mapsto xy$.

In much the same way that the Lie algebra corresponding to a Lie group, studies a neighborhood of the identity, up to first order, we will study functions near the identity up to any order. In our case, the identity is $\mathfrak{m}_1$. Thus, to study functions on G_m up to n-th order, we should look at $k\left[x, x^{-1}\right]/\mathfrak{m}_1^n$, and to study them up to any order, we should take the limit, i.e. the completion by this ideal.

To compute the completion, it is convenient to change variables $s = x - 1$, so that $k\left[x, x^{-1}\right] = k\left[s, (s+1)^{-1}\right]$ and $\mathfrak{m}_1 = (s)$, thus completion is $k[[s]]$. Also the multiplication after change of variables and completion becomes $k[[t]] \to k[[s, u]]$, $t + 1 \mapsto (s+1)(u+1)$ which is the same as $t \mapsto su + s + u$. So, near the identity, the multiplication is specified by an element of $k[[s, u]]$ which is $su + s + u$, called the *multiplicative formal group law*. Note that 0 is a neutral element, and that the law is associative and commutative (since the operation satisfied these properties to begin with.)

In what follows, we axiomatize the resulting structure, similarly to the axiomatization of Lie algebras.

2 Introduction

Definition. Let R be a commutative ring with unit. A (commutative one-dimensional) *formal group law* over R is an element $F(x, y) \in R[[x, y]]$, such that:

1. $F(x, 0) = x = F(0, x)$
2. $F(F(x, y), z) = F(x, F(y, x))$ (associativity)
3. $F(x, y) = F(y, x)$ (commutativity)

We denote the *set of formal group laws* over a ring R by $\mathrm{FGL}(R)$.

Definition. Given an homomorphism $\varphi : R \to S$, and $F \in \mathrm{FGL}(R)$ given by, $F(x, y) = \sum a_{ij} x^i y^j$, we define $\varphi_*(F)(x, y) = \sum \varphi(a_{ij}) x^i y^j$. (This makes $\mathrm{FGL}(\bullet) : \mathrm{Ring} \to \mathrm{Set}$ into a functor.)

Example. The additive formal group law, $F_a(x, y) = x + y$.

Example. The multiplicative formal group law, $F_m(x, y) = x + y + uxy$ for some unit $u \in R$, and specifically $F_m(x, y) = x + y + xy$.

Lemma. *$p(x) \in R[[x]]$ is (multiplicatively) invertible if and only if $p(0) \in R$ is invertible.*

Proof. Let $p(x) = \sum a_n x^n$, and assume $q(x) = \sum b_n x^n \in R[[x]]$ is an inverse to p, i.e. $pq = 1$. By comparing coefficients it follows that $a_0 b_0 = 1$ (so the first part follows), and $\sum_{k=0}^{n} a_k b_{n-k} = 0$. If a_0 is invertible then we can find a suitable q, by defining $b_0 = a_0^{-1}$, and $b_n = -a_0^{-1}\left(\sum_{k=1}^{n} a_k b_{n-k}\right)$ (so the second part follows). □

Lemma. *There exists an element $\iota(x) \in R[[x]]$ called the* inverse *such that $F(x, \iota(x)) = 0 = F(\iota(x), x)$.*

Definition. An *homomorphism* from F to G, two formal group laws over R, is a $f \in R[[x]]$, such that:

1. $f(0) = 0$
2. $f(F(x, y)) = G(f(x), f(y))$

Remark. The definition of an homomorphism between formal group laws, turns the collection of formal group laws over a ring into a category, Also, given a morphism of rings φ, the map φ_* is actually a functor between the corresponding categories.

Lemma. *$f : F \to G$ is (compositionally) invertible (i.e. an isomorphism) if and only if $f'(0)$ is invertible.*

Proof. It is easy to see the first implication. If $f'(0) = 0$, we can show explicitly that there exists a unique g such that $g(f(x)) = x$, and $g'(0) = (f'(0))^{-1}$. From the very same claim, it follows that there exists an h such that $h(g(x)) = x$, it follows that $h(x) = h(g(f(x))) = f(x)$. □

Definition. $f : F \to G$ is a *strict isomorphism* if $f'(0) = 1$.

Example. Over a $\mathbb{Q}$-algebra (where we can divide by $n > 0$), the multiplicative formal group law is strictly isomorphic to the additive formal group law, by $f(x) = u^{-1} \log(1 + ux) = \sum_{n=1}^{\infty} \frac{(-u)^{n-1} x^n}{n}$:

$$\begin{aligned} f(F_m(x, y)) &= u^{-1} \log(1 + uF_m(x, y)) \\ &= u^{-1} \log\left(1 + ux + uy + u^2 xy\right) \\ &= u^{-1} \log(1 + ux)(1 + uy) \\ &= u^{-1} \log(1 + ux) + \log(1 + uy) \\ &= F_a(f(x), f(y)) \end{aligned}$$

(Note that we don't need the u^{-1} to get an isomorphism, but we do need it to get a strict isomorphism.)

Definition. A strict isomorphism from F to F_a is called a *logarithm.*

Lemma. *Let $f \in R[[x]]$ be such that $f(0) = 0, f'(0) = 1$ (i.e. $f(x) = x + \cdots$), then there is a unique formal group law F_f over R whose logarithm is f.*

Proof. The condition of being a logarithm means that $f(F_f(x, y)) = f(x) + f(y)$, or equivalently $F_f(x, y) = f^{-1}(f(x) + f(y))$. The uniqueness is thus trivial, and being a formal group law is also easy to check. □

3 Characteristic 0

Theorem. *A formal group law over a $\mathbb{Q}$-algebra has a logarithm.*

Proof. Let F be such a formal group law, and denote $F_2 = \frac{\partial F}{\partial y}$. Since $F(x, y) = x + y + \cdots$, we know that $F_2(0, 0) = 1$, thus $F_2(t, 0)$ is (multiplicatively) invertible. Since each $0 \neq n \in \mathbb{Z}$ is invertible, we can define the following:

$$f(x) = \int_0^x \frac{\mathrm{d}t}{F_2(t, 0)}$$

We claim that it is a logarithm. We know that $f(0) = 0$ and $f'(0) = \frac{1}{F_2(0,0)} = 1$. It is sufficient to prove that $w(x, y) = f(F(x, y)) - f(x) - f(y) = \sum c_{ij} x^i y^j$ vanishes. First, note that $w(x, 0) = f(F(x, 0)) - f(x) - f(0) =$

$f(x) - f(x) - 0 = 0$ and it follows that $c_{i0} = 0$. If we prove that

$$\begin{aligned} 0 &= \frac{\partial w}{\partial y} \\ &= f'(F(x,y)) F_2(x,y) - f'(y) \\ &= \frac{1}{F_2(F(x,y),0)} F_2(x,y) - \frac{1}{F_2(y,0)} \end{aligned}$$

it follows that $jc_{ij} = 0$, and since each $0 \neq j \in \mathbb{Z}$ is invertible, $c_{ij} = 0, j > 0$, which finishes the proof. Indeed, by associativity, $F(F(x,y),z) = F(x, F(y,z))$, differentiating w.r.t. z at $z = 0$ we get, $F_2(F(x,y),0) = F_2(x,y) F_2(y,0)$ and the result follows. $\square$

4 Characteristic p

Remark. The theorem for characteristic 0 is not true over arbitrary rings.

To see this, we define a notion, that will lead us to the concept of height. Let $F \in \mathrm{FGL}(R)$. We define $[n]_F(x) \in R[[x]]$, called the *n-series* of F, recursively:

$$[0]_F(x) = 0 \qquad [n+1]_F(x) = F\left(x, [n]_F(x)\right)$$

Clearly, for $f : F \to G$ we get $f\left([n]_F(x)\right) = [n]_G(f(x))$.

For F_a we have $[n]_{F_a}(x) = nx$, and by induction for F_m we have $[n]_{F_a}(x) = (1+x)^n - 1$. Consider them over a field of characteristic p, and assume that $f : F_m \to F_a$ is an homomorphism then

$$0 = [p]_{F_a}(f(x)) = f\left([p]_{F_m}(x)\right) = f\left((1+x)^p - 1\right) = f(x^p)$$

which means that f is not invertible, thus F_m and F_a are not isomorphic.

Lemma. *For all n, $[n]_F$ is an endomorphism of F.*

Proof. This amounts to understanding that $[n]_F(x)$ is like nx. It is trivial by definition that $[n](0) = 0$. The addition by induction. For $n = 0$ trivial. Now:

$$\begin{aligned} [n](F(x,y)) &= F(F(x,y), [n-1](F(x,y))) \\ &= F(F(y,x), F([n-1](x), [n-1](y))) \\ &= F(y, F(x, F([n-1](x), [n-1](y)))) \\ &= F(y, F([n](x), [n-1](y))) \\ &= F(y, F([n-1](y), [n](x))) \\ &= F([n](y), [n](x)) \\ &= F([n](x), [n](y)) \end{aligned}$$

$\square$

In what follows in this section, R is an $\mathbb{F}_p$-algebra.

Lemma. *Let $F, G \in \mathrm{FGL}(R)$, and $f : F \to G$ non-trivial. Then $f(x) = g\left(x^{p^n}\right)$ for some n and $g \in R[[x]]$ with $g'(0) \neq 0$, and in particular the leading term of f is ax^{p^n}.*

Proof. If $f'(0) \neq 0$, we are done. Otherwise, we will find a formal group law $\tilde{F}$, and $\tilde{f} : \tilde{F} \to G$, such that $f(x) = \tilde{f}(x^p)$. Since f is non-trivial, and the least non-zero degree is lowered by this process, this process must terminate after a finite amount of stages. So suppose $f'(0) = 0$.

First we claim that $f'(x) = 0$. Deriving $f(F(x,y)) = G(f(x), f(y))$ by y and setting $y = 0$, we get $f'(F(x,0)) F_2(x,0) = G_2(f(x), f(0)) f'(0)$ remembering that $F(x,0) = x, F_2(x,0) = 1, f'(0) = 0$, we conclude that $f'(x) = 0$. Now, write $f(x) = \sum a_n x^n$, from $f'(x) = 0$ it follows that $na_n = 0$ for all n, thus $a_n = 0$ for all $p \nmid n$. So we can define $\tilde{f}$, by $f(x) = \tilde{f}(x^p)$.

Denote by $\varphi : R \to R$ the Frobenius endomorphism $\varphi(x) = x^p$. Define $\tilde{F} = \varphi_*(F)$. It follows that

$$\tilde{f}\left(\tilde{F}(x^p, y^p)\right) = \tilde{f}\left(F(x,y)^p\right) = f(F(x,y)) = G(f(x), f(y)) = G\left(\tilde{f}(x^p), \tilde{f}(y^p)\right)$$

thus $\tilde{f}\left(\tilde{F}(x,y)\right) = G\left(\tilde{f}(x), \tilde{f}(y)\right)$ (since these are just formal power series, so just rename the variables), and it follows that $\tilde{f} : \tilde{F} \to G$ is the desired homomorphism. ☐

Definition. The *height* of $F \in \mathrm{FGL}(R)$ is defined as follows: if $[p]_F(x) = 0$, the height is ∞, otherwise it is the unique $n \in \mathbb{N}$ such that $[p]_F(x) = g\left(x^{p^n}\right)$ with $g'(0) \neq 0$.

Lemma. *The height is an isomorphism invariant.*

Proof. Let $f : F \to G$ be an isomorphism. We've seen that in that case $f([n]_F(x)) = [n]_G(f(x))$. Since f is an isomorphism, $f'(0)$ is a unit, the least non-zero degree is conserved and the result follows. ☐

Theorem. *For each $1 \leq n \leq \infty$ there exists a formal group law F_n of height n.*

Theorem. *Over an algebraically closed field, there is a unique formal group law of each height $1 \leq n \leq \infty$.*

5 The Lazard Ring

Theorem. *There is a ring L, called the* Lazard ring*, and a formal group law over it F_{univ}, called* the universal formal group law*, such that for every ring R the map*

$$\hom_{\mathrm{Ring}}(L, R) \to \mathrm{FGL}(R) \qquad \varphi \mapsto \varphi_*(F_{\mathrm{univ}})$$

is one-to-one and onto. That is, the functor $\mathrm{FGL} : \mathrm{Ring} \to \mathrm{Set}$ *is corepresentable by L.*

Proof. Look at the ring $\tilde{L} = \mathbb{Z}[c_{ij}]$, and $\tilde{F}_{\mathrm{univ}}(x,y) = \sum c_{ij} x^i y^j \in \tilde{L}[[x,y]]$. There are various relations obtained from the definition of a formal group law, e.g. $c_{0j} = 0 = c_{i0}$. Denote by I the ideal generated by these relations, and define $L = \tilde{L}/I$, and $F_{\mathrm{univ}}(x,y) = \sum (c_{ij} + I) x^i y^j \in L[[x,y]]$, which satisfies the definition of a formal group law over L by construction. The map being one-to-one is trivial. Given a formal group law $F(x,y) = \sum a_{ij} x^i y^j$, we can define $\tilde{\varphi} : \tilde{L} \to R$ by $\tilde{\varphi}(c_{ij}) = a_{ij}$. It is clear that $\tilde{\varphi}$ is 0 on I (since the coefficients F satisfy the relations), so that it factors to a map $\varphi : L \to R$, and clearly $\varphi_*(F_{\mathrm{univ}}) = F$, therefore it is onto. ☐

We can define grading on L, by first defining a grading on $\tilde{L}$. Assume that $|x|, |y| = d$, and require that $|F_{\mathrm{univ}}(x,y)| = d$, then $d = \deg(c_{ij}) + di + dj$. It is convenient (specifically for algebraic topology) to choose $d = 2$, thus $|c_{ij}| = 2(i + j - 1)$. It is also true that all relations in the definition of a formal group law compare values of the same degree, thus the grading descends to L. (Also note that $c_{00} = 0$ so it is non-negatively graded.)

Theorem (Lazard)**.** *$L \cong \mathbb{Z}[t_1, t_2, \dots]$ where $|t_i| = 2i$.*

Look at the ring $\mathbb{Z}[b_1, b_2, \dots]$ where $|b_i| = 2i$, and define $f(x) = x + b_1 x^2 + b_2 x^3 + \dots$. We showed before that $F_f = f^{-1}(f(x) + f(y))$ defines a formal group. In the same way that L corepresents formal group laws, $\mathbb{Z}[b_1, b_2, \dots]$ corepresents formal group laws that have a logarithm. Also note that there is a coclassifying map from L for F_f, denoted by $\phi : L \to \mathbb{Z}[b_1, b_2, \dots]$ (compatible with the grading).

Lemma. *$\phi_{\mathbb{Q}} : L \otimes \mathbb{Q} \to \mathbb{Q}[b_1, b_2, \dots]$ is an isomorphism, and in particular surjective.*

Proof. This is precisely the statement that over a $\mathbb{Q}$-algebra every formal group law has a logarithm. ☐

Let I, J be the ideals consisting of elements of positive degree in $L, \mathbb{Z}[b_1, b_2, \dots]$ respectively. It is clear that J/J^2 is a free abelian group with generators b_i so that $\left(J/J^2\right)_{2n} \cong \mathbb{Z}$ (generated by b_n).

Lemma. *ϕ induces an injection $\left(I/I^2\right)_{2n} \to \left(J/J^2\right)_{2n}$, and the image is $p\mathbb{Z}$ if $n + 1 = p^f$, and $\mathbb{Z}$ otherwise.*

In particular it follows that $\left(I/I^2\right)_{2n} \cong \mathbb{Z}$. Choose generators, and lift them to homogeneous $t_n \in I_{2n} = L_{2n}$. This naturally defines a map $\theta : \mathbb{Z}\left[t_1, t_2, \dots\right] \to L$.

Lemma. *θ is surjective.*

Proof. Easy induction on the degrees. Note that we have relation $c_{01}, c_{10} = 1$, so the base case follows. Elements of $\left(I^2\right)_{2n}$ are generated by products of elements of degrees $1 \leq d < 2n$, which are in $\mathrm{im}\theta$ by induction, thus $\left(I^2\right)_{2n} \subset \mathrm{im}\theta$. Since $t_i \in \mathrm{im}\theta$ is a generator of $\left(I/I^2\right)_{2n}$, it follows that $L_{2n} = I_{2n} \subset \mathrm{im}\theta$. ☐

Lemma. *$\psi = \phi\theta : \mathbb{Z}\left[t_1, t_2, \dots\right] \to L \to \mathbb{Z}\left[b_1, b_2, \dots\right]$ is injective, and in particular θ is injective.*

Proof. Since they are torsion-free, it is sufficient to prove that $\psi_{\mathbb{Q}} = \phi_{\mathbb{Q}}\theta_{\mathbb{Q}} : \mathbb{Q}\left[t_1, t_2, \dots\right] \to L\otimes\mathbb{Q} \to \mathbb{Q}\left[b_1, b_2, \dots\right]$ is an isomorphism. $\theta_{\mathbb{Q}}$ is surjective since θ is, $\phi_{\mathbb{Q}}$ was shown to be surjective, thus the composition $\psi_{\mathbb{Q}}$ is surjective. In every degree, the rings are finite dimensional $\mathbb{Q}$-vector spaces, with surjective linear map between them, so it follows that it is an isomorphism in every degree, and thus globally. ☐

Proof of Lazard's theorem. The map $\theta : \mathbb{Z}\left[t_1, t_2, \dots\right] \to L$ was shown to be injective and surjective. ☐

References

[1] Douglas C. Ravenel, *Complex Cobordism and Stable Homotopy Groups of Spheres*, appendix A2.
`http://web.math.rochester.edu/people/faculty/doug/mu.html`
`http://web.math.rochester.edu/people/faculty/doug/mybooks/ravenelA2.pdf`

[2] Douglas C. Ravenel, given by Mike Hopkins, *Complex Oriented Cohomology Theories and the Language of Stacks*.
`http://web.math.rochester.edu/people/faculty/doug/otherpapers/coctalos.pdf`

[3] Jacob Lurie, *Chromatic Homotopy Theory*, lectures 2-3 and 11-14.
`http://www.math.harvard.edu/~lurie/252x.html`

[4] Michiel Hazewinkel, *Formal Groups and Applications*.

[5] Michiel Hazewinkel, *Three Lectures on Formal Groups*.
`http://oai.cwi.nl/oai/asset/2517/2517A.pdf`

[6] nLab, *Height of a Formal Group*.
`https://ncatlab.org/nlab/show/height+of+a+formal+group`